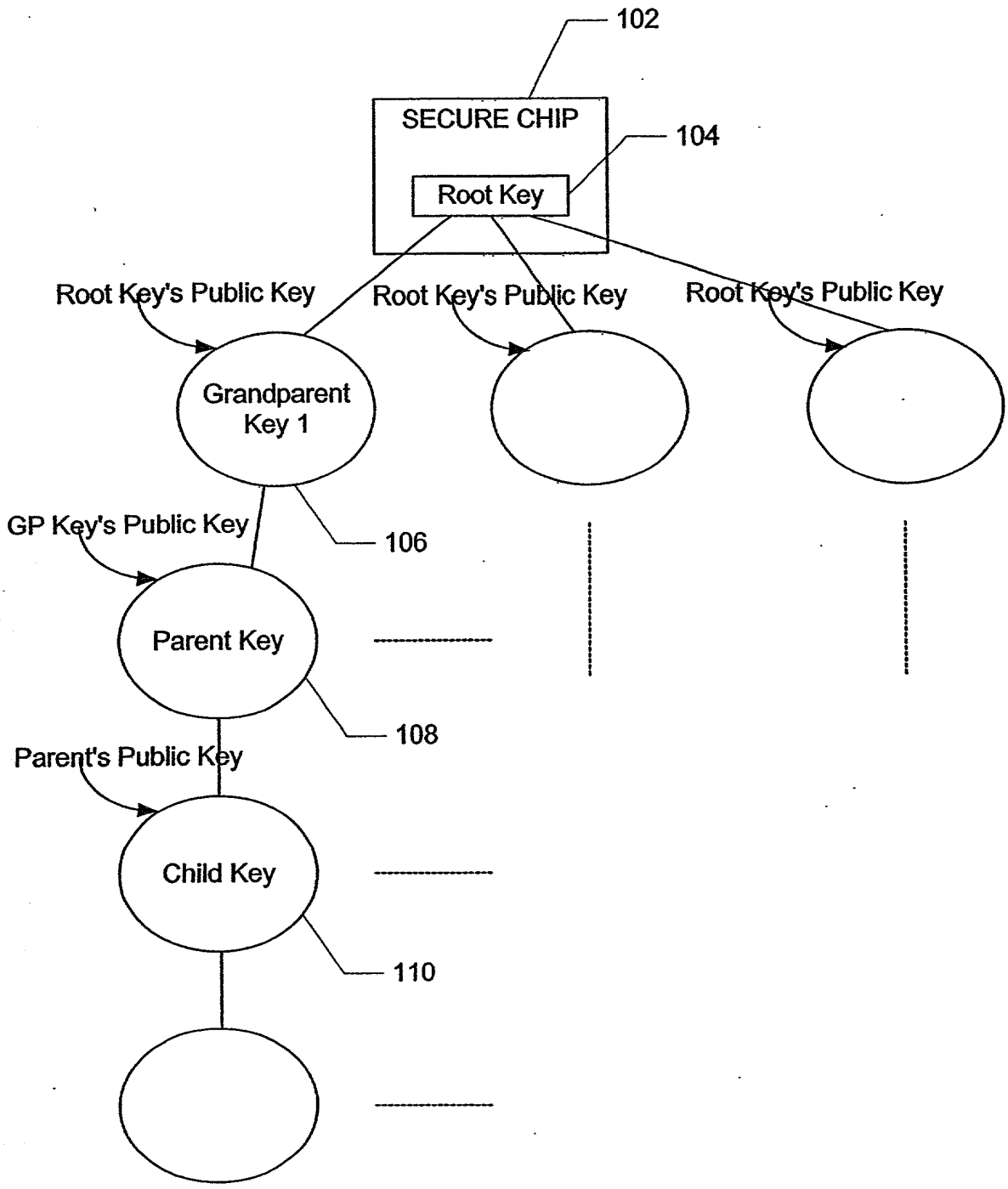

FIG. 1 (Prior Art)

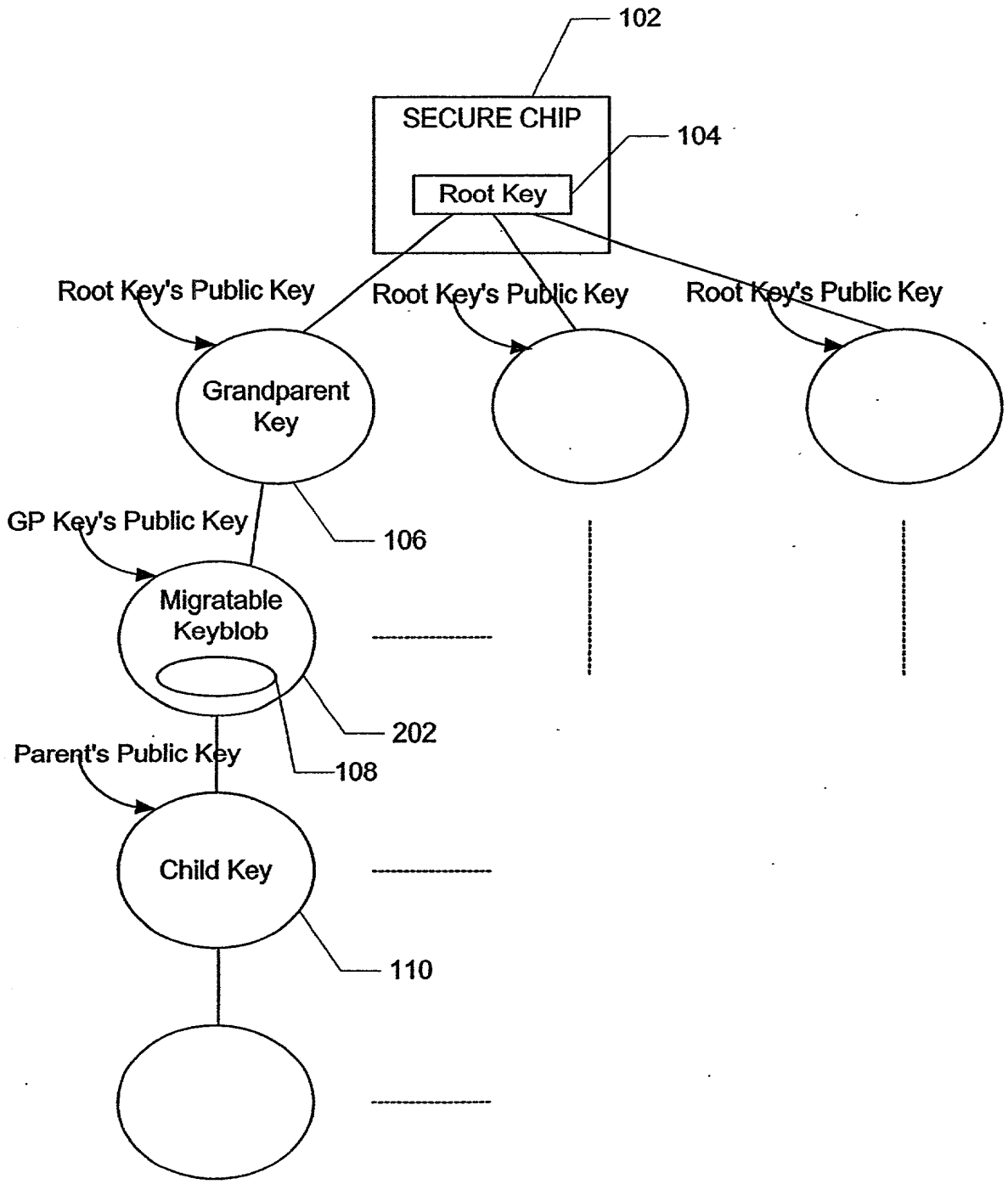
102
SECURE CHIP
104
Root Key
Root Key's Public Key
Root Key's Public Key
Root Key's Public Key
Grandparent Key
GP Key's Public Key
106
Migratable Keyblob
202
Parent's Public Key
108
Child Key
110

FIG. 2

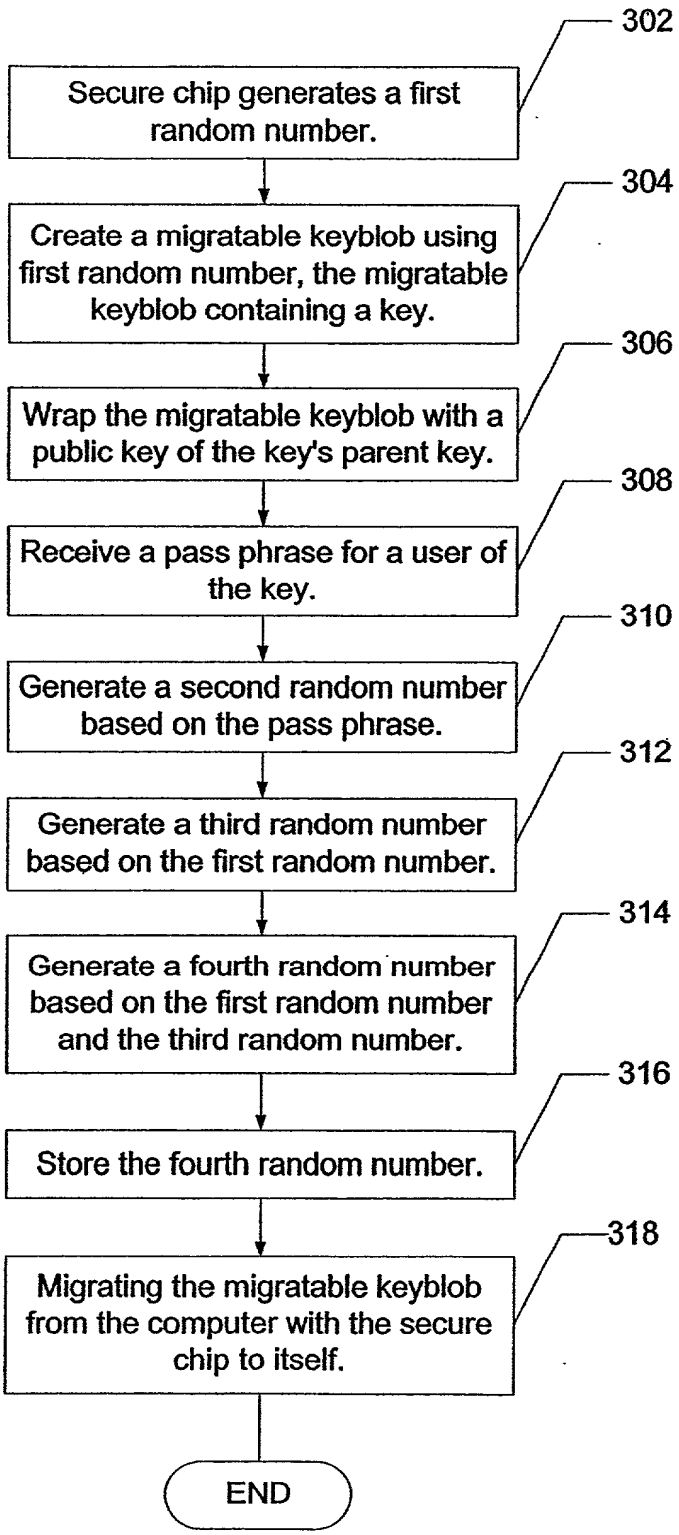
302
Secure chip generates a first random number.
304
Create a migratable keyblob using first random number, the migratable keyblob containing a key.
306
Wrap the migratable keyblob with a public key of the key's parent key.
308
Receive a pass phrase for a user of the key.
310
Generate a second random number based on the pass phrase.
312
Generate a third random number based on the first random number.
314
Generate a fourth random number based on the first random number and the third random number.
316
Store the fourth random number.
318
Migrating the migratable keyblob from the computer with the secure chip to itself.
END

FIG. 3

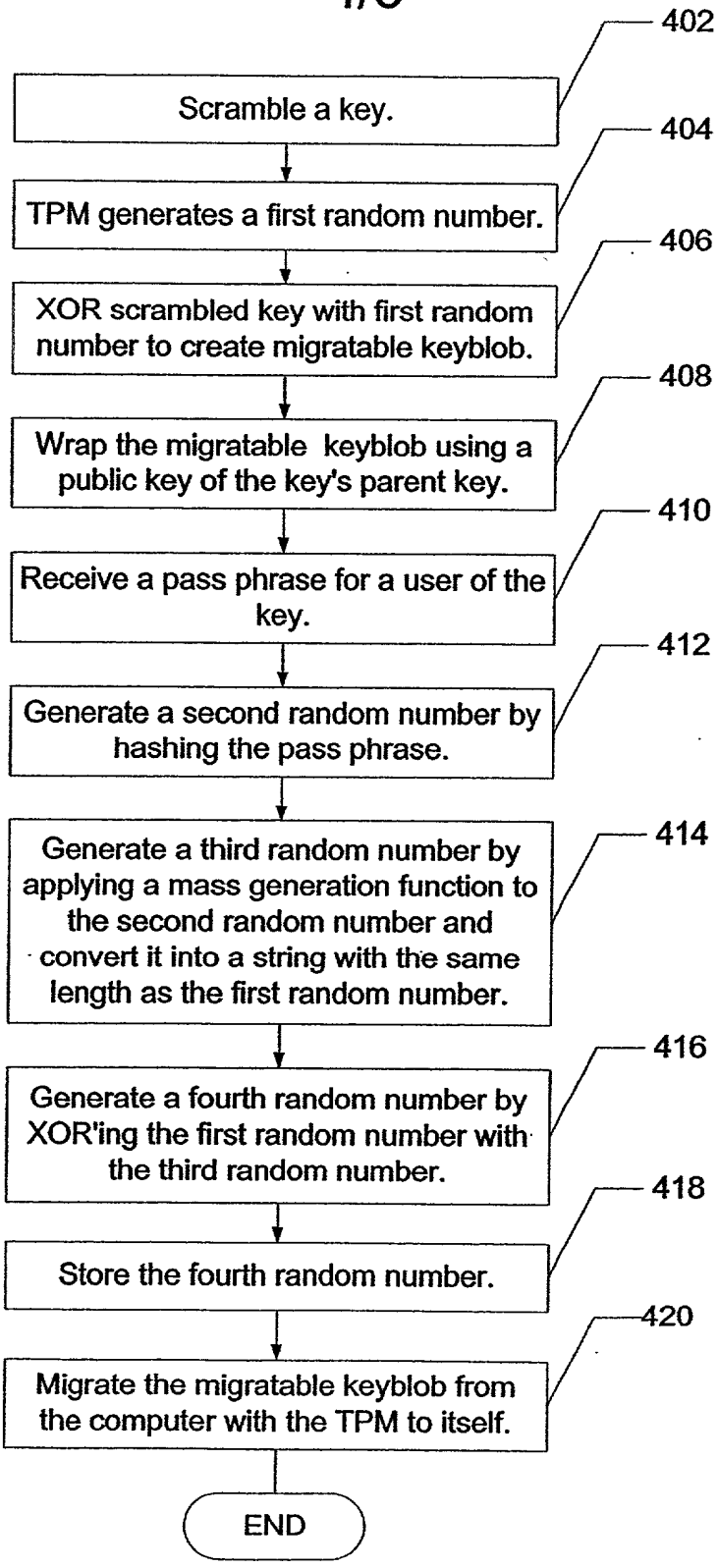
402
Scramble a key.
404
TPM generates a first random number.
406
XOR scrambled key with first random number to create migratable keyblob.
408
Wrap the migratable keyblob using a public key of the key's parent key.
410
Receive a pass phrase for a user of the key.
412
Generate a second random number by hashing the pass phrase.
414
Generate a third random number by applying a mass generation function to the second random number and convert it into a string with the same length as the first random number.
416
Generate a fourth random number by XOR'ing the first random number with the third random number.
418
Store the fourth random number.
420
Migrate the migratable keyblob from the computer with the TPM to itself.
END

FIG. 4

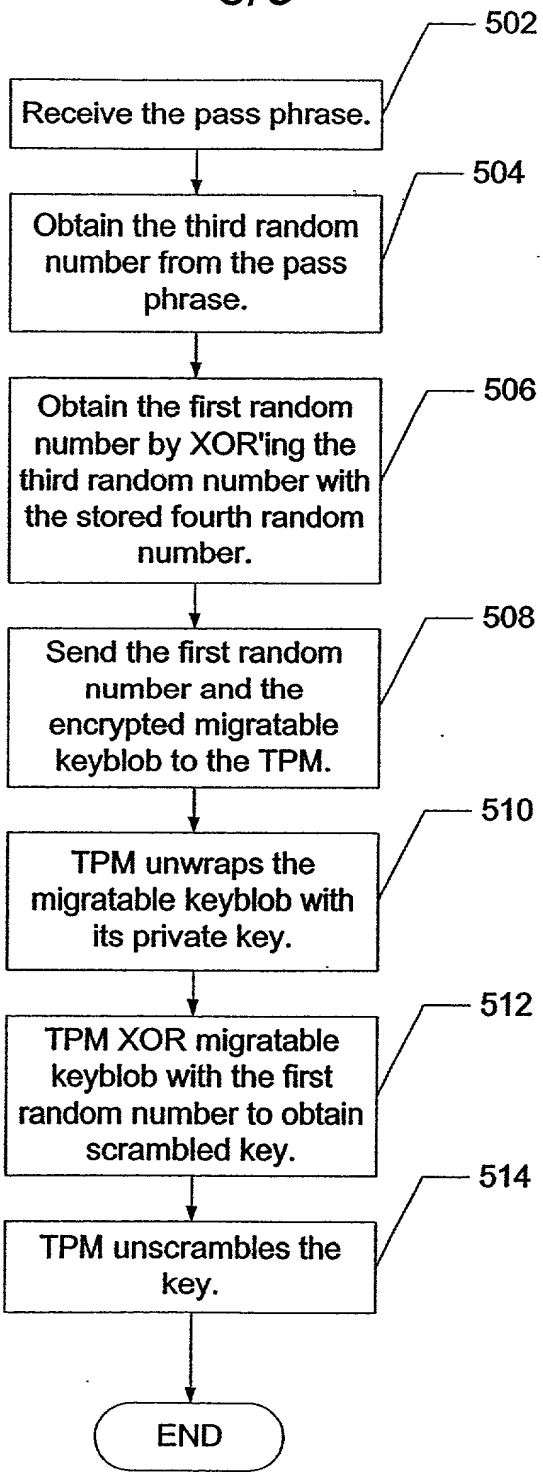
502
Receive the pass phrase.
504
Obtain the third random number from the pass phrase.
506
Obtain the first random number by XOR'ing the third random number with the stored fourth random number.
508
Send the first random number and the encrypted migratable keyblob to the TPM.
510
TPM unwraps the migratable keyblob with its private key.
512
TPM XOR migratable keyblob with the first random number to obtain scrambled key.
514
TPM unscrambles the key.
END

FIG. 5